VŠB – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

BAKALÁŘSKÁ PRÁCE

2011 Peter Haltman

VŠB – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra informatiky

Možnosti replikační topologie Active Directory na platformě Windows Server 2003

Possibilities of Active Directory replication topology running on Windows Server 2003

2011 Peter Haltman

ZADÁNÍ

Cílem práce bude popis replikací, možností jejich konfigurací a služby KCC (Knowlege Consistency Checker) mezi doménovými řadiči Active Directory Windows Server 2003.

Řešení bude zohledňovat následující body:

Možnosti instalace Active Directory pro prostředí různých velikostí s důrazem na logickou i fyzickou strukturu.

Možnosti konfigurace intersite a intrasite replikací, zhodnocení vhodnosti manuální konfigurace replikací.

Analýza replikačního provozu ve virtuální instalaci Active Directory v prostředí alespoň pěti řadičů a více lokací (sites).

Vytvoření názorného tutoriálu pro optimální umístění FSMO rolí Active Directory.

PROHLÁŠENÍ

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně.

Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne ----------

Velmi rád bych zde poděkoval lidem, kteří měli významný vliv na vznik této práce:

Ing. Richardu Biječkovi za inspiraci při výběru bakalářské práce a odborný dohled při její tvorbě.

JUDr. Terézii Haltmanové za zapůjčení hardware pro realizaci bakalářské práce.

ABSTRAKT

Bakalářská práce s názvem Možnosti replikační topologie Active Directory na platformě Windows Server 2003 je rozdělena do dvou základních částí.

Teoretická část se věnuje jednotlivým aspektům replikace, od popisu Active Directory, až po její strukturu. Součástí teoretické části je také postup instalace a popis testovací topologie, která je použita v následující praktické části.

Praktická část se zabývá analýzou replikace, která se dá rozdělit do dvou následujících podkapitol, měření zabývající se časovou jednotkou a měření zabývající se objemem dat.

KLÍČOVÁ SLOVA

Active Directory, síť, intrasite, intersite, replikace, doména, objekt

ABSTRACT

This bachelor work with title Possibilities of Active Directory replication topology running on Windows Server 2003 is divided into two basic parts.

Theoretical part devotes to individual aspects of replication, from describing of Active Directory to its structure. Part of theoretical part is also manual for installation and description of topology, which is used in next practical part.

Practical part includes analysis of replication, which can be split into two following subchapters. Measuring of time and measuring of the size of data.

KEYWORDS

Active Directory, site, intrasite, intersite, replication, domain, object

OBSAH

1 Úvod

Každá firma, která v dnešní době využívá výpočetní techniku, potřebuje přehled a organizaci mezi zaměstnanci, efektivně předávat práci nebo například sdílet firemní data pro potřeby zaměstnanců. Aby taková organizace fungovala, je nelogické, aby počítače, které k této práci využíváme, fungovaly samostatně. Proto již od počátku tvorby operačních systému se myslelo na takové řešení, kde by počítače spolu komunikovaly a díky tomu si mohly efektivně předávat úlohy nebo sdílet data.

Cílem této bakalářské práce je vytvořit analýzu replikačního provozu pro určení průtoku dat v síti. Metod měření je celá řada, já se proto pokusím začínajícímu administrátorovi jak číselně, tak graficky představit průřez jednotlivými metodami s výčtem jejich předností a možnostmi použití.

Bakalářskou práci využijí jak začínající administrátoři, kteří se seznámí se základními prvky Active Directory (viz kapitola 2), pokročilejší uživatelé, kteří už mají vlastní doménu vytvořenou, ale chtějí nastavit síťové cesty replikace (viz kapitola 5), tak i uživatelé, kteří se zajímají o analýzu replikace (viz kapitola 6), ve které získají veškeré informace o objemu dat, které v sítí díky replikaci protékají.

Účelem této bakalářské práce je seznámit zájemce o implementaci Active Directory se základními prvky administrace, které jim systém nabízí.

2 STRUKTURA ACTIVE DIRECTORY

Active Directory si můžeme představit jako databázi, která shromažďuje informace o objektech v celé síti, jako jsou uživatelé, počítače nebo tiskárny.

Abych mohl pojem Active Directory vysvětlit podrobněji, musím se nejdříve zmínit o pojmu LDAP, ze kterého Active Directory vychází. LDAP je definovaný protokol pro ukládání a přístup dat na serveru. Každá položka je uložena formou záznamu[1] do adresářového serveru. Adresářový server slouží k uchování různých typů dat. Díky tomu, se hojně využívá pro práce s informacemi o všech objektech ve struktuře databáze. Protokol LDAP funguje na bázi klient-server. Spolu s protokolem je jeho součástí i fáze, kde se musí uživatel autentizovat[2]. To se děje přihlášením skrze zařízení za pomocí jména (pro rozeznání jednotlivých uživatelů) a hesla (pro bezpečný přístup uživatelů do sítě).

Z předcházejícího odstavce proto můžeme odvodit, že Active Directory je implementací protokolu LDAP, který byl vytvořen společností Microsoft pro použití v systémech Windows. Díky tomu můžeme centralizovat informace o uživatelích, počítačích nebo tiskárnách do databáze.

Active Directory si můžeme rozdělit do dvou pohledů. Z hlediska geografického rozmístění – fyzická struktura a z hlediska organizačního – logická struktura.

2.1 LOGICKÁ STRUKTURA

Logická struktura se skládá z těchto prvků: objekty, organizační jednotky, domény, doménové větve a doménové lesy.

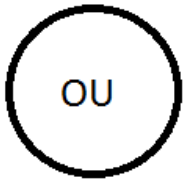
Obr. 2.1.1 základní objekty logické struktury

Objekty jsou základním prvkem logické struktury, mezi ně můžeme zařadit všechny uživatelské účty, počítače a tiskárny. Každý objekt v Active Directory je unikátně definován kombinací atributů a jeho hodnoty. Atribut definuje možné hodnoty, které můžou být s objektem spojeny. Každý objekt, například uživatel, je založen na objektu třídy uživatel,

[1] pod pojmem záznam si můžeme představit souhrn atributů -jméno atributu a jeho hodnota
[2] je proces ověření identity subjektu

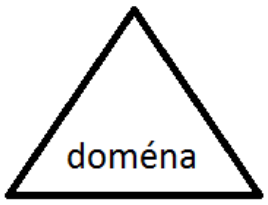
počítač je pro změnu založen na objektu třídy počítač a tiskárna je založena na objektu třídy tiskárna. Třídy objektů a atributy jsou souhrnně označovány jako schéma.

Organizační jednotky[3] jsou kontejnerem, do kterého můžeme vkládat objekty. Jako příklad, lze uvést vytvoření organizační jednotky uživatelů, kteří jsou rozděleni podle umístění v budově, odděleních nebo jiných požadavků správce. Díky tomuto řešení je snadnější spravovat objekty v Active Directory. Je také možné vytvořit hierarchii organizačních jednotek, kdy jedna organizační jednotka obsahuje další organizační jednotky. Slouží také pro delegaci oprávnění nebo aplikaci politik. Organizační jednotky značíme kolečkem.



Obr. 2.1.2 značení organizační jednotky

Domény jsou podstatou celé logické struktury Active Directory. Nabízí tři funkce: chovají se jako administrační hranice pro objekty, pomáhají řídit bezpečnost pro sdílené zálohy a slouží jako stavební kámen replikace pro objekty. Doména je kolekcí objektů, které sdílejí adresářovou databázi, bezpečnostní politiku a vztahy důvěry s ostatními doménami. Domény značíme trojúhelníkem.



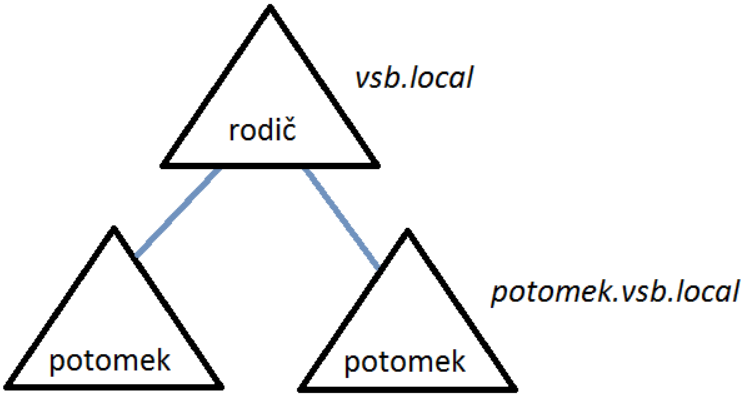
Obr. 2.1.3 značení domény

Objekty v každé doméně jsou uloženy ve specifickém oddílu databáze Active Directory. Servery[4] ukládají samotné kopie (nebo repliky) doménových oddílů. Tyto repliky se navzájem automaticky aktualizují, což znamená, že pokud se některá z nich modifikuje, dojde po čase k rozšíření této informace na ostatní doménové řadiče. Díky tomu zůstává doména konzistentní.

Domény jsou navzájem uspořádány do hierarchické struktury, ty se nazývají doménové větve. Následující vložené domény do stromu, se stanou potomkem kořene domény. Doména,

[3] V původním názvu Organizational unit, zkratka OU
[4] V doméně je nazýváme doménové řadiče

na kterou je navázán potomek se pak nazývá rodičem. Potomek může na sebe navazovat další potomky. Aby však byl určitý řád v názvosloví, je zapotřebí, aby potomek obsahoval jméno rodiče. Název domény musí být unikátní, aby byl rozeznán v systému DNS. Kupříkladu jméno domény je vsb.local, proto když vytvoříme potomka v doméně, je zapotřebí, aby obsahoval jak jméno rodiče, tak jméno samotného potomka např. potomek.vsb.local. Les je instance Active Directory s jednou nebo více doménami.



Obr. 2.1.4 pojmenování rodičů a potomků v doméně

Doménový les se skládá z jedné nebo více větví. První doména v lese se nazývá kořenová doména. Název celého lesa se odkazuje na jméno první domény, která v tomto lese vznikla.

2.2 FYZICKÁ STRUKTURA

Fyzická struktura je zcela oddělená od struktury logické, vytváří pak ale jednotný celek v práci s Active Directory. V logické struktuře spravujeme uživatele, skupiny a zdroje sítě, kdežto fyzická struktura nám umožňuje optimalizovat toky dat v síti. Fyzická struktura například definuje, kdy a kde budou nastávat replikace nebo ve kterém čase bude síť přístupná pro uživatele. Základní části ve fyzické struktuře jsou tyto tři prvky – sítě[5], linky a doménové řadiče[6]. Každý doménový řadič slouží jako uložiště dat a nástroj k replikaci, obsahuje databázi informací, které se v síti replikují. Doménový řadič se váže pouze na jednu instalaci Windows Serverů, není tedy možné, abychom na jednom počítači provozovali více domén. Doménový řadič je takto omezen z důvodu politik a bezpečnosti. U větších firem se počítá, že bude jejich síť obsahovat více, než jeden doménový řadič. Těm se pak mohou přidělovat různé role ve správě sítě, kdy jeden funguje jako DHCP server, druhý bude mít za úkol DNS, třetí bude sloužit jako úložiště dat a tak dále. Je také možné, aby jednu službu provádělo více řadičů

[5] Častěji se používá anglicky název site
[6] Doménovým řadičem je počítač, na kterém běží služba Active Directory s operačním systémem Windows Server.

zároveň nebo naopak, kdy jeden řadič slouží více účelům. Tato problematika se dá shrnout do tématu FSMO role, o které se zmiňuji v následující kapitole.

Síť je skupina dobře[7] propojených počítačů. Úmyslně však nepíši žádnou doporučovanou rychlost. Záleží na samotné potřebě domény, některá doména si vystačí s propojením v rychlostech řádu kilobajtů za sekundu, některé sítě si vyžádají megabajty za sekundu. Jakmile je síť vytvořena, doménové řadiče ihned vzájemně komunikují. Není zapotřebí službu nijak spouštět, v základní instalaci jsou nastaveny hodnoty pro základní použití k replikaci. Active Directory sítě a služby slouží k tomu, aby se vytvářela co nejmenší latence[8] v síti. Latence značí časovou složku, za kterou se doménové řadiče budou replikovat.

Při vytváření domény je nezbytné pomyslet na správné nastavení jak logických jednotek, tak i fyzických. Firma může mít pobočky na celém světě, ty jsou v různých časových pásmech, je pak příhodné naplánovat vhodný čas pro replikaci domény mezi doménovými řadiči. Pomyslete také na to, že v průběhu pracovních hodin by mělo docházet k minimální komunikaci mezi doménovými řadiči a to z důvodu přístupnosti doménových řadičů v průběhu pracovní doby. Tento jev se může projevit u slabších pracovních stanic. Rozmístění sítí neznamená to, že sítě musí mít mezi sebou geograficky závažnou vzdálenost, několik sítí zároveň může fungovat i v jediné budově.

2.3 INSTALACE DOMÉNY

Pro správnou instalaci domény je zapotřebí dodržet některé kroky, které je potřeba řádně promyslet.

- Výběr správného hardware – už při samotném nákupu počítače bychom si měli dávat pozor, aby všechny hardwarové komponenty byly kompatibilní se systémem Windows Server. Každý větší výrobce komponent by měl mít ovladače komponent certifikovány od společnosti Microsoft, jen tak můžeme předejít případným problémům pro správné fungování domény.
- Výběr operačního systému – Microsoft nabízí několik edicí Windows Server 2003, některé jsou vhodné pro menší firmy, některé servery se zaměřují na provoz internetových stránek. Proto je dobré konzultovat předem s vedoucím, k jakým účelům bude náš server určen.
- DNS, NetBIOS – před instalací domény je nutné v systémech Windows Server 2003 doinstalovat program pro řízení DNS (překlad IP adres na jména a naopak). Tento prvek se vyžaduje pro všechny počítače, které jsou v doméně. Pokud naše doména nebude „2003 native“, čili bude nejenom obsahovat servery s operačním systémem Windows Server 2003, ale také operační systémy Windows NT je nutné zprovoznit prvek NetBIOS, který je takovým předchůdcem DNS.

[7] Jinak řečeno vysokorychlostně
[8] Reakční čas

- Umístění serveru – server by měl být umístěn v prostředí, kde se budou vyskytovat pouze správci domény, tímto odepřeme přístup standardních uživatelů k serveru. Server se musí také ochránit před prostředím, kde může dojít k požáru nebo jiným nehodám. Obojí se dá zařídit dle následujících kroku, server umístíme do místnosti, ke které budou mít přístup pouze správci, ještě pro větší bezpečnost server umístíme do uzamykatelného racku. Ten musí být dobře větraný a chráněný před okolím, není vhodné v těchto případech šetřit penězi, pamatujte na to, že na serveru budou uloženy všechny informace firmy.
- Heslo na obnovu adresářové struktury – při instalaci domény budeme dotázáni vytvořit heslo pro obnovu adresářové struktury, toto heslo by mělo splnit několik podmínek, musí být silné, což znamená, že heslo by mělo obsahovat malá a velká písmena, čísla a znaky zároveň, heslo by nemělo být totožné s heslem administrátora. Pokud si nedokážete heslo zapamatovat, napište si jej na papírek a vložte do firemního nebo bankovního trezoru.
- Záloha dat – hned ze startu je vhodné myslet i na zálohy systémových složek, neexistuje žádný univerzální návod, jak často zálohu vytvářet, záleží vždy na požadavcích firmy, některá si vystačí se zálohou na týden, některá tuto zálohu vytváří každé 2 hodiny, s častou zálohou počítejte i s větším vytížením sítě. Záložní pásky nebo harddisky je vhodné umístit mimo budovu a to z důvodu bezpečnosti, pokud dojde k požáru, data máte bezpečně zálohovány.

Prvotní instalace systému Windows Server 2003 je obdobná jako u standardních systémů od firmy Microsoft. Hned zezačátku je důležité zmínit, že při instalaci systému Windows Server 2003 je potřeba vybrat formátování disku v NTFS. To z toho důvodu, že jedině tento formát podporuje šifrování dat a je nedílně spojen se službou Group Policy[9]. Po instalaci systému je také důležité nainstalovat DNS službu, která je nedílnou součástí fungování Active Directory. Tuto službu je možné doinstalovat skrze nabídku Start -> Ovládací panely -> Přidat a odebrat programy. Při instalaci je vhodné si nejdříve pojmenovat název stanice pro snadnější detekci v síti. Pro instalaci služby Active Directory napíšeme do příkazového řádku příkaz „dcpromo“.

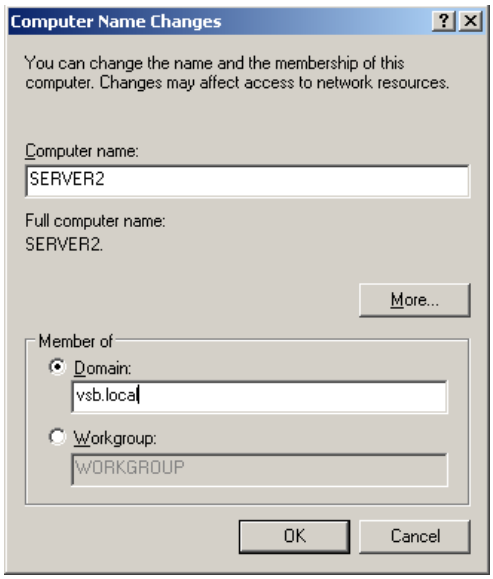
V první části průvodce máme na výběr z možností vytvoření nové domény nebo vložení do domény již vytvořené. Jelikož doména není vytvořená, zvolíme možnost pro vytvoření domény nové. Poté se zadá jméno domény. Ta by měla mít podle pravidel dva řády[10]. Ukázková Active Directory bude mít název vsb.local[11]. Po nutném restartu počítače je doména připravena. Následně je zapotřebí nakonfigurovat síťové připojení pro správné fungování domény a

[9] Není součástí bakalářské práce, jedná se však o službu, která poskytuje nastavit objektům Active Directory práva pro vstup do složek, pro přístup k tiskárnám, je také možnost nastavit skripty po přihlášení do domény.
[10] Kolik má doména řádu je snadné rozpoznat, jsou oddělené tečkou.
[11] Název local je vhodný z toho důvodu, kdy budeme chtít rozlišovat naši AD od názvu internetových stránek.

rozeznání[12] počítačů v doméně. Pro tyto účely byla pro doménový řadič vybrána IP adresa 10.0.0.1 s maskou podsítě 255.255.255.0. Úlohu DNS serveru přenecháme této stanici.

Obr. 2.3.1. nastavení IP adresy, masky podsítě a upřednostňovaného DNS serveru

Pro připojení do již existující domény je postup podobný jako při instalaci Active Directory na serveru1. Nejdříve je vhodné přejmenovat stanici a v níže zobrazeném okně zároveň zadat, do které domény se bude připojovat po následném restartu systému.



Obr 2.3.2 přejmenování stanice a přidání člena do domény „vsb.local“

[12] V základu je v systémech Windows Server 2003 nastaveno získání IP adresy od DHCP serveru.

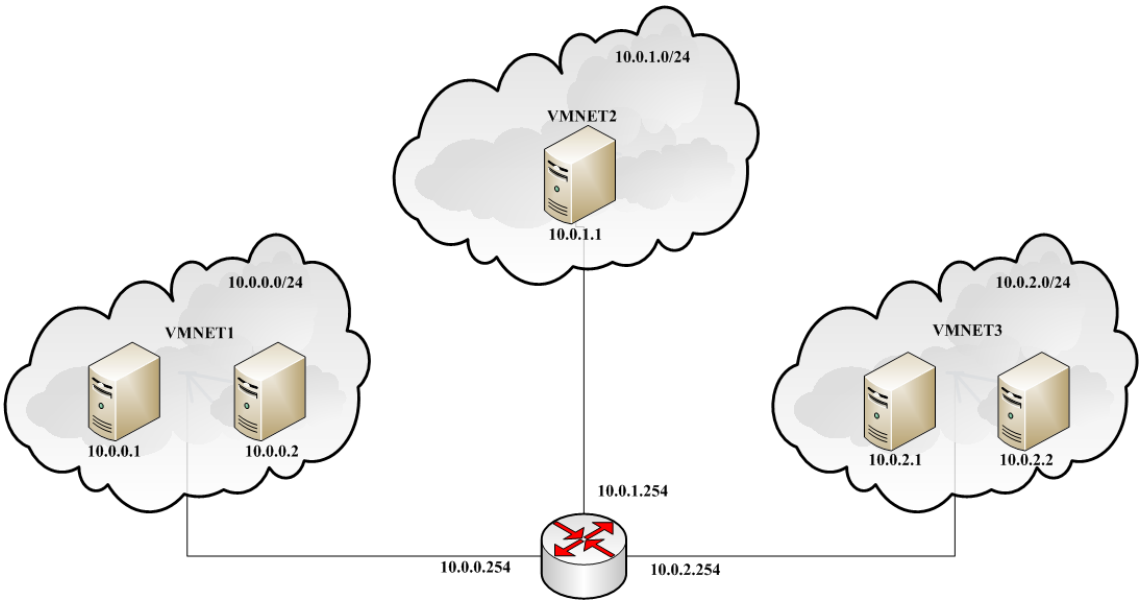
V každém počítači je třeba definovat upřednostňovaný DNS server, který slouží jako výchozí zdroj pro poskytování DNS záznamu. Pro tyto účely byly vybrány následující parametry zbývajících serverů, které budou v topologii spadat pod SERVER1.

Po vyžadovaném restartu, zařadíme SERVER2 do domény příkazem „dcpromo“ v příkazovém řádku, jako to bylo u stanice SERVER1. Protože doména byla vytvořena v předchozím kroku následující servery, budeme jen přidávat do již existující domény.

Testovací doména je rozdělena do tří geografických oblastí. V první oblasti se nachází hlavní server1 se serverem2. Na serveru1 je spuštěna služba DNS, kterou využívá celá doména. Tuto oblast jsem pojmenoval VMNET1. V další oblasti se nachází jediný doménový řadič – server3, ten se nachází ve VMNET2. V poslední oblasti VMNET3 se nacházejí stejně jako ve VMNET1 dva doménové řadiče a to server4 a server5. Topologii jsem vytvořil za pomocí programu VMWare Player, kdy každý server obsahuje jednu virtuální síťovou kartu. Router je vyřešen za pomocí virtualizace Windows Serveru 2003, který spravuje 3 síťové karty. Každá ze síťových karet má na starosti jednu ze sítí VMNET.

Jméno stanice	**Síť**	**IP adresa**	**Maska podsítě**	**Výchozí brána**	**Upřednostňovaný DNS server**
SERVER1	VMNET1	10.0.0.1	255.255.255.0	10.0.0.254	1.2.3.4
SERVER2	VMNET1	10.0.0.2	255.255.255.0	10.0.0.254	1.2.3.4
SERVER3	VMNET2	10.0.1.1	255.255.255.0	10.0.1.254	1.2.3.4
SERVER4	VMNET3	10.0.2.1	255.255.255.0	10.0.2.254	1.2.3.4
SERVER5	VMNET3	10.0.2.2	255.255.255.0	10.0.2.254	1.2.3.4

Tab. 2.3.1 síťové nastavení doménových řadičů v testovací doméně



Obr 2.3.3 topologie sítě - každý VMNET značí jednu virtuální síť

3 FSMO ROLE

Každé větší firemní prostředí by mělo obsahovat více doménových řadičů. Neexistuje, aby jeden řadič prováděl více služeb a to z důvodu výkonu a bezpečnosti. Proto vznikly FSMO role - Flexible Single Master Operations.

FSMO role slouží k tomu, aby se serverové služby rozmístily na doménové řadiče tak, aby byly co nejpřístupnější a nejzabezpečenější.

3.1 DĚLENÍ FSMO ROLÍ

Hlavní server schématu (Schema Master)

Jak už název napovídá, hlavní server schématu spravuje všechny modifikace ve schématu Active Directory. Jakmile je schéma změněno, dojde k replikaci na další doménové řadiče.

Schema Master se vyskytuje jediný v celém lese.

Hlavní názvový server domény (Domain Naming Master)

Hlavní názvový server má na starosti přidávání a odebírání všech domén v lese. Jinak řečeno jeho úlohou je zaručovat jedinečnost názvů domén v doménové struktuře.

Domain naming master se vyskytuje jediný v celém lese.

Hlavní server relativních identifikátorů (RID Master)

Každý objekt Active Directory má přiřazen unikátní identifikační číslo. Nevznikne tak problém, že by dva rozdílné objekty v doméně měly stejný RID (relative ID). Tento problém nevznikne díky tomu, že server má na starosti generování RID mezi doménové řadiče.

RID Master se vyskytuje jediný v celé doméně.

Hlavní server infrastruktury (Infrastructure Master)

Má velmi důležitou roli v doménové struktuře s více doménami. Jsou-li uživatelé přidáni jako členové struktury do druhé domény, je Infrastrucure Master zodpovědný za údržbu všech aktualizací ve vzdálené doméně.

Infrastructure Master se vyskytuje jediný v celé doméně.

Emulátor primárního řadiče domény (PDC Emulator)

Už v názvu se vyskytuje důležitá informace – emulátor. Pokud jsou v naší doméně řadiče se systémem Windows NT 4, je nezbytné, aby síť obsahovala záložní řadiče. PDC emulator je zodpovědný za jejich aktualizaci. Také zodpovídá za přijímání žádostí o změnu hesla v doméně. Zadá-li uživatel nesprávné heslo, je kontaktován PDC emulator a ten kontroluje, jestli heslo uživatele nebylo před žádostí o přihlášení změněno na jiném řadiči domény. Je také zodpovědný za synchronizaci času v celé doméně.

PDC Emulator se vyskytuje jediný v celé doméně.

3.2 OBECNÁ PRAVIDLA PRO FSMO ROLE

- PDC emulator se umísťuje do sítě, kde se nachází nejvíce uživatelů.
- Schema master se umísťuje do sítě, která obsahuje nejvíce řadičů domény.
- RID master se umísťuje co nejblíže PDC emulátoru, dokonce může být na stejném serveru, také na místo, kde dochází k častému vytváření objektů.
- Domain naming master se umísťuje zároveň s globálním katalogem, často se dává na stejný doménový řadič, který má roli Schema Master.

4 ODDÍLY ACTIVE DIRECTORY

Každá databáze Active Directory se skládá z několika oddílů: doménový oddíl, konfigurační oddíl, aplikační oddíl a schéma. Proto replikace neprobíhá na úrovní celé Active Directory, která by byla těžkopádná jak pro systém, tak pro síť, ale právě na úrovni těchto oddílů.

- Doménová vrstva obsahuje repliky [13]všech objektů v doméně. Doménová vrstva se replikuje do všech doménových řadičů domény.

- Konfigurační vrstva obsahuje topologii lesu. Jinak řečeno obsahuje konfiguraci objektů sítě a služeb.

- Schéma, obsahuje všechny třídy a atributy, které objekty mohou obsahovat.

Nepovinnou položkou v Active Directory jsou oddíly aplikační. Ty obsahují objekty, které nemají žádnou souvislost se zabezpečením Active Directory a jsou využívány jednou či více aplikacemi.

[13] Jinak řečeno kopie

5 REPLIKACE

Replikace je proces kopírování datových objektů[14] a udržení konzistence dat v databázovém systému Active Directory. Změny, které aplikujeme na jednom z doménových řadičů, se nejprve uloží lokálně na harddisk. Po určité[15] době oznámí zbývajícím řadičům změnu dat, toto však platí pouze uvnitř sítě. Zde je však důležité upozornit, že ostatní doménové řadiče jsou pouze informovány o změně, podle algoritmů se systém rozhodne, zdali si replikaci vyžádá ihned nebo bude nadále čekat. Data by pak vyžadoval ve větším a kompletnějším balíku, díky tomuto algoritmu se síť příliš nezatíží. Mohlo by se také stát, že si replikaci vyžádal v nevhodnou dobu, kdy je doménový řadič zatížen správou ostatních služeb. Díky tomu replikace zajišťuje, aby uživatel měl přístup k aktuálním datům, a zároveň chrání dostupnost služeb, které doménový řadič nabízí. Celá komunikace popsaná výše probíhá mezi doménovým řadičem, na kterém byla změna provedena a na nejbližším[16] z řadičů. Ostatní řadiče jsou postupně informovány o 3 sekundy později. Pokud máme například v síti 4 řadiče, bude proces [17] trvat 21 sekund.

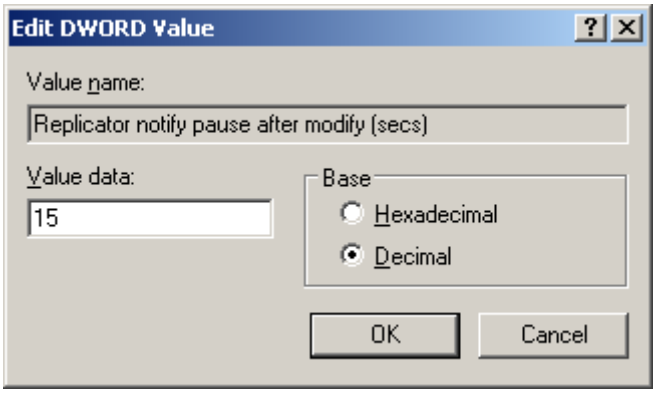
5.1 INTRASITE REPLIKACE

Intrasite replikace probíhají uvnitř jedné sítě. Jednotlivé sítě si můžeme představit jako pobočky nebo patra v budově. Důležitým parametrem je rychlost vnitřní sítě, neměla by být vytvořena architektura, která by v sobě obsahovala pomalé propojení doménových řadičů. Proto v rámci finančních možnostech firmy je vhodné, na této síťové položce nešetřit. Je vhodné také myslet do budoucích let, kdy firma může expandovat a rychlost sítě, která nám může momentálně vyhovovat, nemusí už být dostatečná pro budoucí použití.
U intrasite replikací máme možnost nastavit si v registrech dobu, za kterou bude doménový řadič notifikovat ostatní doménové řadiče o změně v jeho databázi. Tento parametr je umístěn:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parametres

Tento klíč není v registrech defaultně vytvořen, proto se musí vložit klíč nový. Nová DWORD [18]hodnota má jméno „Replicator notify pause after modify (secs)“. Tomuto klíči zadáme hodnotu, je možnost si vybrat mezi dvěma číselnými soustavami – hexadecimální nebo decimální. Po přidání je zapotřebí operační systém restartovat. Právě tuto hodnotu budu často používat při testování možností v replikaci.

[14] Jak bylo uvedeno výše, mezi objekty se řadí všichni uživatelé, počítače nebo tiskárny.
[15] Původní hodnota je nastavena na 15 sekund.
[16] Záleží na geografickém uložení, neboli intra site.
[17] Od změny v Active Directory po poslední notifikovaný řadič.
[18] Zkratka double word, je standardním datatypem v jazyku C, na 32 bitovém operačním systému má tato hodnota velikost 32 bitů, na 16 bitovém operačním systému má tato hodnota velikost 16 bitů.



Obr. 5.1.1 změna prodlevy notifikace v registrech systému.

Je důležité upozornit také na to, že hodnota může mít různou velikost na různých doménových řadičích, tam kde je zapotřebí okamžitě informovat ostatní řadiče o změně tuto hodnotu nastavíme nižší v řádech jednotek sekund, počítejte však s tím, že daný doménový řadič bude mít vyšší nároky na síť. Naopak pokud se jedná o doménový řadič, kde data nemusí být často aktualizována, nastavíme tuto hodnotu vyšší. Ve srovnání s operačním systémem Windows Server 2000 byla tato hodnota v původním stavu nastavena na 5 minut oproti 15 sekundám v systémech Windows Server 2003. Zde je jasně vidět, že v průběhu pár let se znatelně zvýšily nároky pro replikaci jako takovou.

5.2 INTERSITE REPLIKACE

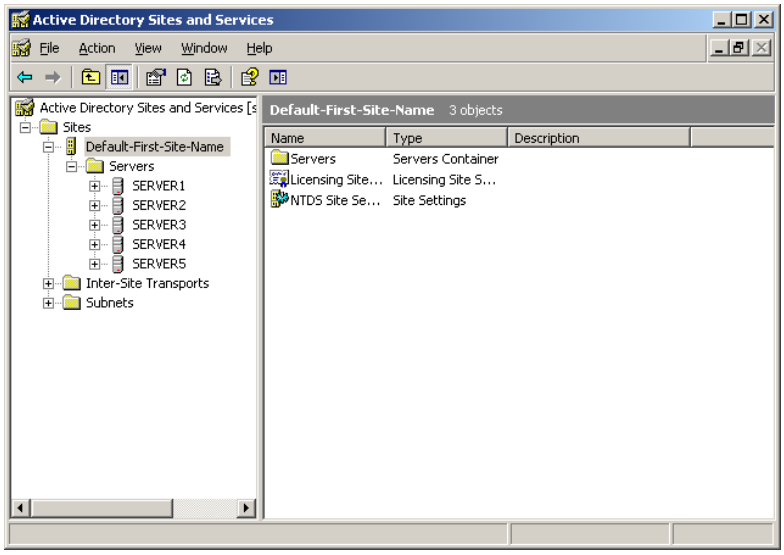
Intersite replikací můžeme nazývat jakoukoliv replikaci, která probíhá mezi dvěma nebo více sítěmi. Klasickým rysem těchto sítí je jejich pomalejší propojení oproti propojení, které je použito v intra sítích. V porovnání vnitřní sítě jsou napojeny v síti v rychlostech 100MBit/s, 1GBit/s nebo 10GBit/s[19]. Naproti tomu stojí sítě, které jsou vzdáleny někdy i několik desítek tisíců kilometrů, pro propojení takové sítě využíváme standardních služeb providerů. Oproti domácímu připojení linky, která může být v agregaci a nespolehlivá bývá častým problémem cena připojení, 1MBit/s může stát měsíčně i několik desítek tisíců, záleží na výběru providera, jeho nabízených služeb a spolehlivosti. Z předchozího příkladu je vidět, že připojení mezi sítěmi může být i několikanásobně pomalejší, proto je důležité soustředit se na co nejefektivnější nastavení této části sítě.

[19] Tyto rychlosti jsou standardem, jaký můžeme objevit i v domácích počítačích, síťové karty které jsou integrovány na základních deskách počítačů. Počítače oproti tomu mají jiné požadavky a síťové karty jsou napojovány do volného slotu základní desky, důvod je jediný, pokud dojde k selhání síťové karty je možnost rychlejší výměny jediné komponenty.

Pro správu intersite spojení využijeme integrovanou aplikaci Windows Server 2003, kterou lze nalézt pod sekcí Start v nabídce Nástroje administrátorů. Služba se jmenuje Služba a sítě Active Directory[20].

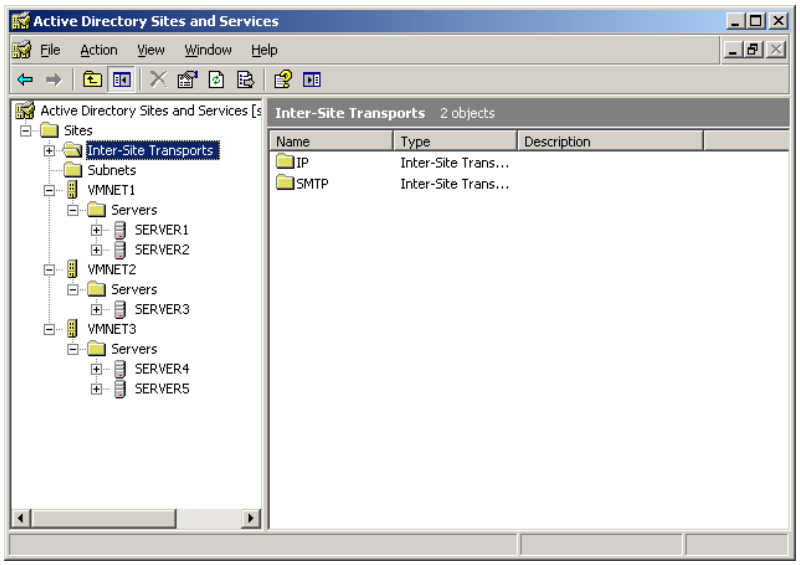
Prostředí aplikace má shodnou filozofii rozložení komponent jako zbývající aplikace, které jsou součástí balíčku pro administrátory. V základu jsou všechny doménové řadiče přidány do sítě, která má specifický název „Default-First-Site-Name“, tu je vhodné ponechat, v případě špatného nastavení některého ze spojení. Pořád bude fungovat toto defaultní, které je automaticky nakonfigurováno systémem. Toto nastavení však počítá s tím, že všechny doménové řadiče se vyskytují na jediném místě.

Pro vytvoření replikace slouží příkaz „New site“. Je vhodné, aby byla vždy podřazena pod IP protokol, který má název DEFAULTIPSITELINK, ten je automaticky generován a není potřebné vytvářet si vlastní nastavení tohoto protokolu. Je vhodné zadávat názvy lokací, kterou síť bude obsluhovat, jako například jména států, krajů. Pokud jsme rozdělili budovu do několika sítí, je vhodné zadat číslo patra popřípadě kód oddělení. Předejdeme tak případným problémům, kdy nebude fungovat linka korektně, a my nebudeme schopni najít jméno lokace z důvodu nevhodného pojmenování. V následujícím kroku je zapotřebí vložit do nově vzniklé sítě doménové řadiče, které do této sítě náleží.



Obr. 5.2.1 rozšířená nabídka sítě „Default-First-Site-Name“ s přehledem serverů, které obsahuje.

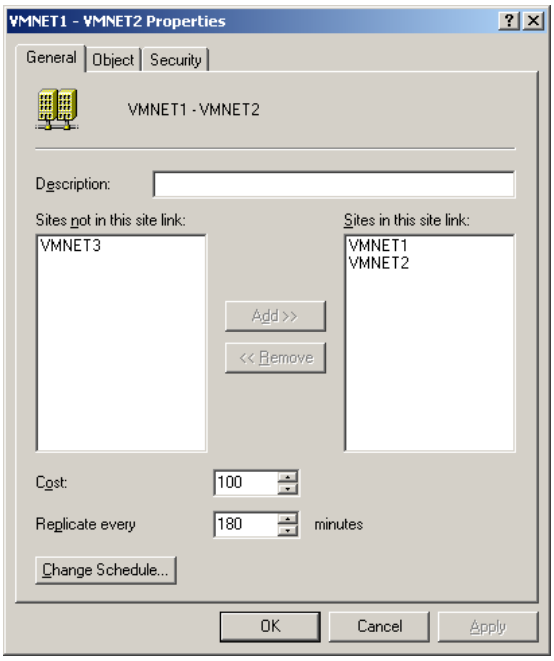
[20] V originálním názvu pojmenované jako Active Directory sites and services.



Obr. 5.2.2 nově vytvořené sítě, podle návrhu ze strany 9

Důležitým aspektem bude konfigurace propojení mezi těmito sítěmi. Propojení mezi těmito sítěmi je nazváno sitelink, ten nalezneme v sekci Inter-Site transports. Je rozdělen podle protokolů, které jsou v replikaci použity. Pro replikaci objektů se využívá IP protokol nebo SMTP protokol, ten se však v praxi nepoužívá. Pro účely bakalářské práce využiji pouze IP protokol. V nabídce IP lze nalézt možnost vytvořit New Site Link, poté se vyberou sítě, mezi kterýma chceme nastavit konfiguraci. Je doporučováno vybírat vždy pouze dvě sítě pro lepší přehled v komunikaci a mít také více možností při optimalizaci replikačního procesu. Jméno doporučuji vybrat ve formátu z „lokace“ do „lokace“, díky tomu později najdeme snadněji síť, kterou chceme spravovat. Je důležité podotknout, že nastavované replikační spojení je vždy jednosměrné, což znamená, že je rozdíl lokace1 – lokace2 a lokace2 – lokace1.

Po vytvoření nové linky jsou nastaveny základní hodnoty. Mezi možnosti nastavení patří – cena, periodika replikace a časový rozvrh, kdy se má replikace provádět.



Obr. 5.2.3 nastavení sitelink s původními hodnotami

Cena linky, jinak také jako priorita, se kterou se bude linka používat. Čím je cena nižší, tím větší má prioritu a naopak. Můžeme si například představit situaci, kdy mezi dvěma sítěmi jsou fyzicky dvě linky, jedna je vysokorychlostní, která se používá jako hlavní linka, druhá linka, která má nižší přenosovou rychlost může sloužit jako záložní. Aby systémy Windows Server tyto linky rozeznaly, nastavíme jim rozlišnou cenu. Primárně se bude používat linka vysokorychlostní, té nastavíme nižší číslo ceny, u záložní linky nastavíme číslo vyšší, ta se tak využije jen v tom případě, že dojde k poruše vedení linky primární.

Kolonka replikace má jasnou úlohu, jedná se o časovou jednotku, kdy v každé periodě odešle cílovému řadiči všechny změny, které se provedly v daném časovém intervalu. V základním nastavení se replikace provede každé 3 hodiny. My si můžeme vybrat, jak často se bude provádět, pokud replikace chceme provádět častěji, nastavíme logicky nižší časový interval, počítejte však s tím, že linka bude více datově zatížena. Zde si však můžeme dovolit časový interval snížit. V datovém toku nebudou rozdíly tak razantní a to z toho důvodu, že se je na administrátorovi, jestli bude chtít přenášet data v celku nebo je rozdělí na časové úseky.

Rozvrh slouží jako další možnost jak replikaci řídit. Uvnitř sítě není tak velký problém[21], v takové síti může proběhnout replikace i několikrát v průběhu pár minut. Základem celého snažení je provádět replikaci co nejčastěji, aniž bychom ovlivnili vytížení sítě. Rozvrh slouží k tomu, aby se v časovém plánu nastavily hodiny, kdy může probíhat replikace tak, aby se prováděla v dobu, kdy nejsou zaměstnanci na pracovišti. Například víme, že pracovní doba v jedné pobočce je od 9:00 do 15:00, druhá pobočka má stejnou pracovní dobu, ale je v jiném

[21] Počítá se s tím, že síť bude mít vysokorychlostní propojení.

časovém pásmu, proto nastavíme čas replikace tak, aby se prováděla mimo pracovní dobu obou poboček zároveň. Tím zajistíme, že síť se v té době bude věnovat jen replikaci objektů v Active Directory. Vše je však pouze o nalezení rovnováhy mezi konzistencí dat a vytížení sítě.

6 ANALÝZA REPLIKAČNÍHO PROVOZU

V analýze replikačního procesu jsou zásadní dva parametry, na které je měření zaměřeno.

- Čas – důležitý parametr, ze kterého se dá mnoho vyčíst, v praxi je velice důležité vědět, jak dlouho budou trvat různé fáze replikace.
- Množství dat – existuje nepřímá souvislost s časovou jednotkou, čím větší množství dat je zapotřebí replikovat, tím déle bude trvat proces. Z tohoto údaje lze také vyvodit optimální velikost datové linky, kterou budeme potřebovat pro replikaci mezi dvěma sítěmi.

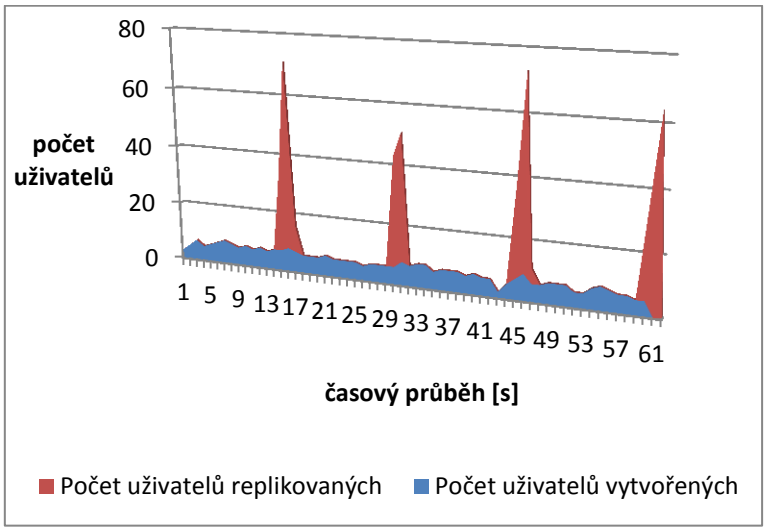
6.1 ČASOVÁ SLOŽITOST

Pro měření jsem využil různé nástroje. V první části měření jsem se zajímal o průběh intrasite replikace. U ní je důležitý časový parametr. Pokud bychom tvořili hromadné operace pro vkládaní nových objektů do databáze, nebude vhodnější vyčkat na notifikaci, až po vložení všech objektů? Tím pádem by se nezatěžovala síť průběžně a ostatní doménové řadiče by v průběhu mohly nabízet jiné služby. Nebo právě naopak, bude vhodnější objekty postupně replikovat? Tím pádem rozložíme zatížení sítě i zatížení procesorů do kratších časových úseků. Jsou však systémy Windows Server 2003 natolik inteligentní, aby při hromadné změně databáze raději vyčkali na kompletní změnu databáze a neměly tak na starosti dvě úlohy zároveň?

Pro testy, které jsou zaměřené na časový parametr replikace, je vytvořena sada skriptů, které zapisují časové údaje o vytvoření objektu a jeho následné replikace na další řadič. Nejvhodnější pro tyto účely jsem využil jazyka Visual Basic Script. Tento skriptovací jazyk byl vytvořen společností Microsoft, je vhodný pro práci v databázích Active Directory z toho důvodu, protože jeho součástí jsou nástroje pro práci s Active Directory. Není zapotřebí instalovat další plugin. Ten je totiž zakomponován v systémech již od dob Microsoft Windows 95.

Na prvním doménovém řadiči jsou vytvářeny objekty, na druhém doménový řadič sleduje, za jak dlouho se objekty replikují na jeho stanici.

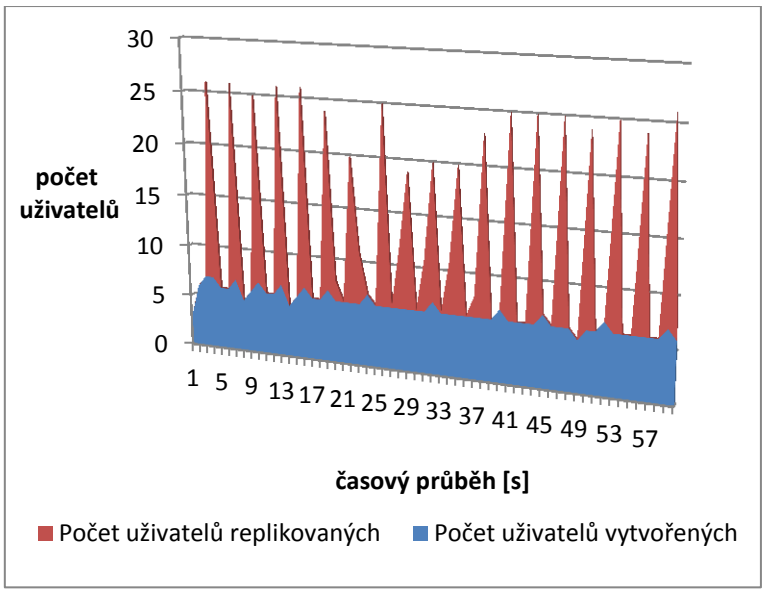
V prvním testu je testováno základní nastavení Active Directory, objekt se vytváří pravidelně každých 100 milisekund, notifikace na další řadič je nastavena na 15 sekund.



Graf 6.1.1 notifikace řadiče po 15 sekundách

Jak jde vyčíst z grafu, Active Directory nečekala na vytvoření všech objektů, ale průběžně odesílala kopie do času notifikace vytvořených. První doménový řadič v té chvíli měl na starosti dvě úlohy, zaznamenával nově vytvořené objekty do databáze a odesílal replikace objektů na ostatní doménové řadiče. V našem případě objekty v té chvíli odesílal pouze na doménový řadič s číslem 2, protože další doménové řadiče jsou v jiných sítích a těm je odeslána notifikace až posléze. Po dalších 15 sekundách odeslal nově vytvořené objekty mezi časovým úsekem 15. a 30. sekundy. Toto chování bylo stejné v celém průběhu časové osy.

V následujícím testu jsem zkrátil notifikaci na 3 sekundy, zbytek testovacích podmínek jsem ponechal na původních hodnotách.

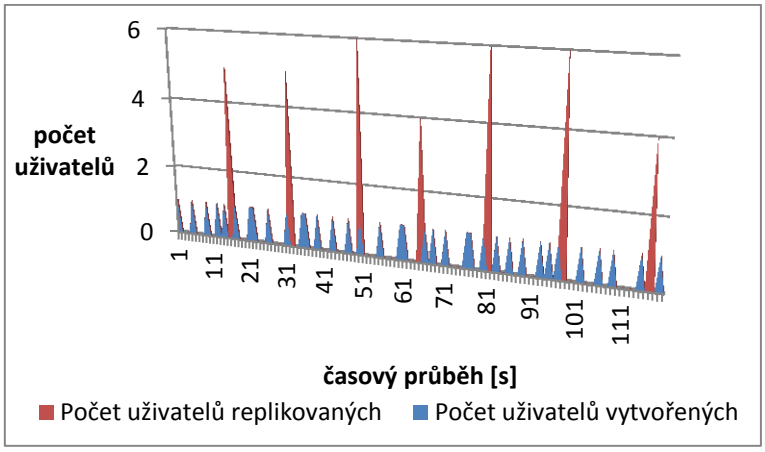


Graf 6.1.2 notifikace řadiče po 3 sekundách

Jak lze vyčíst z výše uvedeného grafu, výsledek je zcela jasný, replikace probíhala ve stejné režii, jako v předcházejícím případě, což znamená, že systém nijak nevyčkal na kompletní změnu v databázi a neodeslal řadičům konečný výsledek.

Předchozí pokusy byly vytvořeny tak, aby pravidelně vkládali objekty do databáze, co se však stane, pokud tyto objekty budeme vkládat v náhodném čase? Pro tento typ testu jsem vytvořil další sadu měření.

V následujícím testu probíhá vkládání nového objektu v časovém rozmezí jedné až pěti sekund.

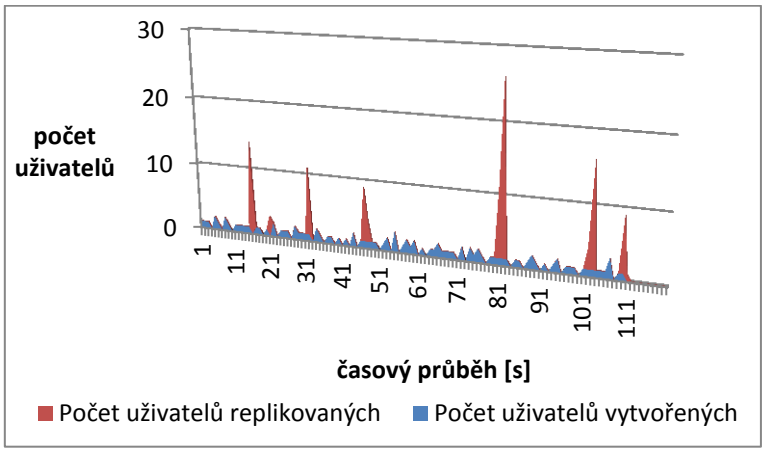


Graf 6.1.3 náhodné vytváření objektu v rozmezí 1-5 sekund

Na výše znázorněném grafu výše lze vidět, jak algoritmus replikace probíhá. Na prvním doménovém řadiči se objekty vytvářejí, jakmile uběhne 15 sekund[22], řadič o tomto průběhu dá vědět ostatním doménovým řadičům v doméně a data se rozešlou. Bohužel ani v tomto testu se neprovedlo žádané chování, kdy očekávám inteligentní chování od systému, který by odesílal objemnější data v delších časových intervalech, než je nastaveno.

Pro poslední test z této řady jsou vytvářeny objekty v různém časovém rozpětí a to od 0,1 sekundy až po 2 sekundy.

[22] Defaultní hodnota pro notifikaci ostatních doménových řadičů



Graf 6.1.4 náhodné vytváření objektu v rozmezí 0,1-2 sekundy

Na grafu výše je uvedena replikace, která oproti předcházejícímu testování vytváří ve velice krátkých intervalech objekty, které po 15 sekundách odesílá na sousední řadič. Díky značně vyššímu zatížení procesoru docházelo při tomto měření k anomáliím, které vedly k zavádějícím výsledkům. Přibližně v 66. sekundě nedošlo k replikaci objektů vytvořených. Procesor byl v tomto momentě na svém maximálním výkonu. Proto přeskočil jeden interval replikace a všechny objekty vytvořené v rozmezí mezi 51. a 81. sekundou replikoval v následující dávce, proto došlo ke skokovému náskoku červené linie v grafu.

6.2 DATOVÁ NÁROČNOST

Další velice důležitou otázkou replikace je její síťové zatížení z pohledu objemnosti dat. Objem dat je nepřímo spojen s časovou jednotkou, čím více jsou objemnější data, tím déle potrvá jejich replikace na ostatní doménové řadiče. Proto je důležité, aby replikace byla tak častá a objemná, aby zbytečně nezatěžovala síť, na druhou stranu nesmí existovat tak dlouhé prodlevy, aby uživatelé nemuseli dlouze čekat na aktuální data.

Pro tento druh měření je využit program Wireshark, který patří mezi špičku monitoringu v síti. Sledovat se budou jednotlivé prvky přenosu v síti, které mezi různými zařízeními mohou proběhnout. V nastavení programu je zapotřebí vytvořit filtr pro sledování datových toků replikace, řadiče si mezi sebou posílají také data, které s replikací nesouvisí, jako je například informace z DNS serveru, díky tomu by mohly být výsledky zavádějící. Z výsledků testů získáme více informací, za prvé zjistíme objem datových toků a také to, jestli se objem dat přímo úměrně zvyšuje s množstvím objektů replikovaných.

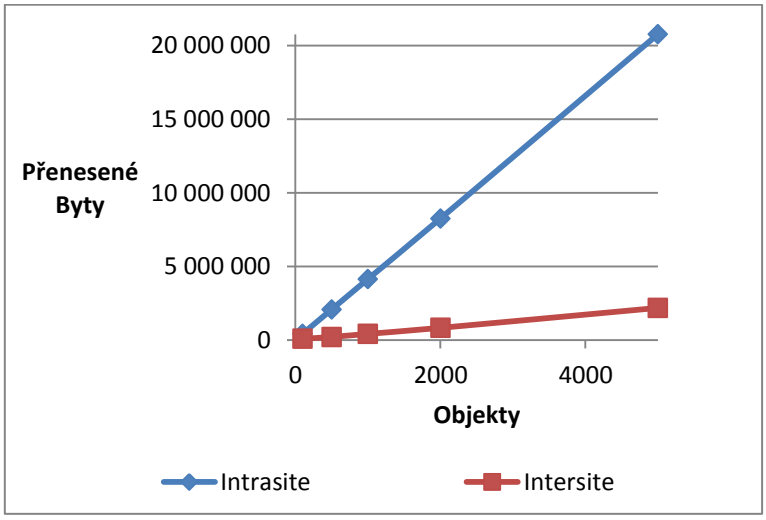
Doménový řadič, na kterém se objekty vytvářely má IP adresu 10.0.0.1, dalším doménovém řadičem ve stejné síti má IP adresu 10.0.0.2 a doménový řadič, který se řadí do jiné

sítě má IP adresu 10.0.2.2. Při tvorbě objektu se vytvářela pouze jeho existence, která se skládala jen z atributu cn[23].

Zdroj	Cíl	Množství objektů	Velikost [B][24]
10.0.0.1	10.0.0.2	100	422 887
10.0.0.1	10.0.2.2	100	79 246
10.0.0.1	10.0.0.2	500	2 073 545
10.0.0.1	10.0.2.2	500	206 754
10.0.0.1	10.0.0.2	1000	4 140 300
10.0.0.1	10.0.2.2	1000	413 408
10.0.0.1	10.0.0.2	2000	8 248 913
10.0.0.1	10.0.2.2	2000	822 062
10.0.0.1	10.0.0.2	5000	20 766 618
10.0.0.1	10.0.2.2	5000	2 177 286

Tab. 6.2.1 výsledky z testování objemu dat

Z tabulky lze také vyčíst, že při replikaci, která se provádí mezi sítěmi, dochází ke komprimaci dat. Po přepočtu se dá zjistit, že dochází ke komprimaci na 1/10 původní velikosti dat. To je sice výhodné pro replikaci mezi sítěmi, na druhou stranu komprimace si vyžádá také větší režii procesoru. To je také důvod, proč se komprimace nevyužívá k replikaci mezi doménovými řadiči v intra síti. Jelikož k intra replikaci[25] může docházet co 10 sekund, nebylo by pro Active Directory výhodné co deset sekund data komprimovat, odesílat a na druhém řadiči provádět jejich dekompresi.



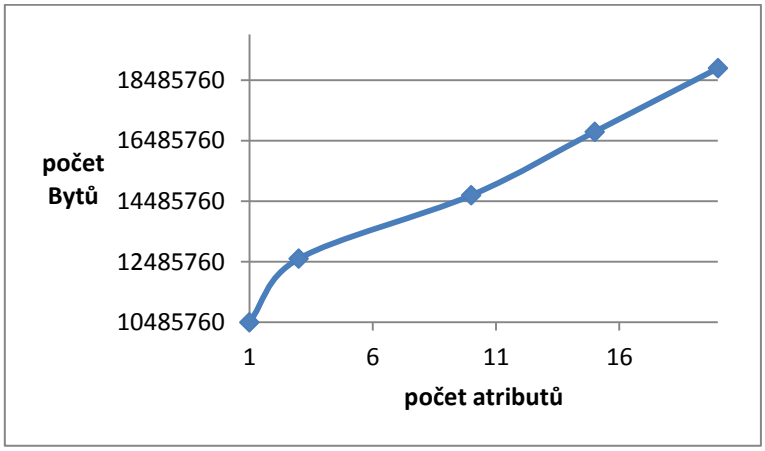
Graf 6.2.1 lineární datový růst k množství atributů

[23] Common name – základní atribut pro každý objekt uživatele, jedná se o jeho jedinečné označení v Active Directory.
[24] 8 388 608 b ~ 1 048 576 B = 1024 kB = 1 MB
[25] Minimální časová prodleva v inter replikaci je 15 minut.

Zajímavým ukazatelem z provedeného testu je množství dat k množství replikovaných objektů. Z níže uvedeného grafu je jasně vidět, že s množstvím replikovaných objektů lineárně roste množství dat k jeho replikaci. Důležitým faktorem je také sklon v grafu, je jasně vidět, že intrasite replikace rostou přibližně desetkrát rychleji oproti replikaci intrasite.

V poslední části analýzy při práci s Active Directory je důležitý faktor, který udává růst dat s rostoucím počtem atributů k objektu. Všechny objekty, mezi které řadíme všechny uživatele, počítače a tiskárny jsou ukládána na jednotném místě do souboru ntds.dit, díky tomu tak snadno můžeme sledovat velikost Active Directory na jednom místě.

Při testu je pokaždé vytvářeno 5000 objektů, ke kterým je přidáván různý počet atributů. V reálném provozu firmy většinou přidávají k objektům 15-20 atributů.



Graf 6.2.2 grafický poměr atributů k množství dat

Po následném výpočtu [26]kdy vydělíme velikost souboru počtem uživatelů, získáme zajímavé hodnoty.

Počet atributů	Počet bytů	Velikost objektu [B]
1	10485760	2097
3	12582912	2516
10	14680064	2936
15	16777216	3355
20	18874368	3774

Tab. 6.2.2. velikost dat k počtu atributů

[26] Je počítáno s tím, že v Active Directory se nenacházejí žádné další objekty, které by výsledek mohly zkreslovat.

Z výše uvedené tabulky získáme tyto hodnoty, pokud bude objekt obsahovat jediný[27] atribut, získáme velikost jednoho objektu přibližně 2,1 kB. Pokud však vytvoříme objekt, který bude v sobě obsahovat 20 atributů, získáme tak skoro dvojnásobnou velikost a to 3,8 kB. Pokud tedy chceme získat odpověď na otázku, kolik si jeden atribut vezme místa na harddisku, získáme hodnotu přibližně[28] 0,09 kB. Tato hodnota je nízká, pokud však v databázi vytvoříme 5000 objektů, které budou mít každý po 20 atributech, dostáváme se k hodnotě skoro 19 MB, což už může být pro replikaci velký balík dat.

[27] Nepočítá se atribut cn, který slouží jako unikátní id objektu v celé databázi Active Directory
[28] V tomto případě nerozeznávám různé datové typy, jako jsou například string, integer, date apod.

7 ZÁVĚR

Hlavním bodem této bakalářské práce bylo blíže se seznámit s replikační topologií na platformě Windows Server 2003. Cílem mé bakalářské práce je, aby správce věděl, přesný postup při tvorbě sítě na bázi Windows.

Replikace mezi doménovými řadiči probíhá v několika fázích, každou vrstvu Active Directory je možnost přizpůsobit podmínkám firmy. S datovou náročností sítě není spojena jenom replikace samotná. Je zapotřebí se zamyslet také nad tím, že ve standardní síti probíhá větší množství datových přenosů jako je internetový přenos, předávání výsledků DNS a speciální protokoly, které si mezi sebou rozesílají aplikace mimo Active Directory.

Tato práce je koncipována jako příručka pro začínající administrátory v operačním systému Windows Server 2003. Naleznou zde nejdůležitější analýzy spojené s objemem dat, který je zásadní otázkou při replikaci v síti. Metod měření existuje celá řada (podkapitoly 6.1 a 6.2), proto jsem vybral ty, které v praxi budou nejužitečnější. Při měření také došlo k anomáliím, které vedly k nepřesným výsledkům. Hardware mého počítače neměl dostatečný výkon pro měření časové jednotky replikace (viz graf 6.1.4). Hodnota je zkreslena z důvodu nedostatečně výkonného procesoru, který má své hranice.

Z výsledků měření je čitelné několik parametrů. Pokud se jedná o replikaci ve vnitřní síti (viz graf 6.2.1), zde dochází ke značné síťové zátěži po celou dobu. U replikace mezi sítěmi je toto hledisko zcela zanedbatelné, pokud máme dostatečně rychlou linku. Pro oba předcházející případy je však jedno společné – vytvořit ideální podmínky pro pracovní prostředí, kde uživatel nebude omezován z důvodu replikace a data zároveň budou v celé síti konzistentní.

LITERATURA

[1] Mistrovství v Microsoft Windows Server 2003, Petr Šetka, Computer Press, 2003

[2] Active Directory: Optimální postupy a řešení problem, Brad Price, Computer Press, 2005

[3] Microsoft Windows Server 2003: Velký průvodce administratora, Charlie Russel, Computer Press, 2005

[4] Active Directory: Kapesní rádce administratora, William Stanek, Computer Press, 2009

[5] Implementace a správa Active Directory, Robbie Allen, Grada Publishing, 2005